日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２８日

出願番号
Application Number: 特願２０００－４００６７０

出願人
Applicant(s): 日本ビクター株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　９月２５日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１　３０８７００５

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: December 28, 2000

Application Number: 2000-400670

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

September 25, 2001

Commissioner,
Japan Patent Office

Kozo Oikawa

Number of Certification: 2001-3087905

【書類名】　特許願

【整理番号】　412001491

【提出日】　平成12年12月28日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/08

G06F　9/06

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　猪羽　渉

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　上田　健二朗

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　黒岩　俊夫

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　日暮　誠司

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　守隨　武雄

【電話番号】　045-450-2423

【手数料の表示】

【予納台帳番号】　003654

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ伝送方法、伝送媒体、及びコンテンツ受信方法

【特許請求の範囲】

【請求項１】

コンテンツの再生を許可することを示すコンテンツ再生許可情報を生成し、

生成された前記コンテンツ再生許可情報に少なくとも基づき鍵情報を生成し、

生成された前記鍵情報を元に前記コンテンツを暗号化し、

前記暗号化されたコンテンツと、前記暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを併せて伝送する、

ことを特徴とするコンテンツ伝送方法。

【請求項２】

コンテンツの再生を許可することを示すコンテンツ再生許可情報に少なくとも基づき生成された鍵情報に基づいて暗号化されたコンテンツと、

前記暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報と、

を伝送することを特徴とする伝送媒体。

【請求項３】

コンテンツの再生を許可することを示すコンテンツ再生許可情報に少なくとも基づき生成された鍵情報に基づいて暗号化されたコンテンツと、その暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを受信して、前記暗号化されたコンテンツを再生するコンテンツ受信方法であって、

受信した前記暗号化されたコンテンツと前記伝送日時情報とを記憶し、

記憶された前記暗号化されたコンテンツに対する再生要求がなされた時点からその暗号化されたコンテンツを復号するための鍵情報を生成する時点までの間における日時に関する再生日時情報を得、

記憶された前記伝送日時情報と、前記再生日時情報と、前記暗号化されたコン

テンツの再生許可期限情報とに基づき、前記暗号化されたコンテンツの再生を許可することを示すコンテンツ再生許可情報を生成し、

生成された前記コンテンツ再生許可情報に少なくとも基づき前記鍵情報を生成し、

記憶された前記暗号化されたコンテンツを、生成された前記鍵情報を元に復号する、

ことを特徴とするコンテンツ受信方法。

【請求項４】

請求項３記載のコンテンツ受信方法において、

前記再生許可期限情報は予め設定されていることを特徴とするコンテンツ受信方法。

【請求項５】

請求項３記載のコンテンツ受信方法において、

前記再生許可期限情報は外部から供給される情報に基づき設定されることを特徴とするコンテンツ受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化され記憶されたコンテンツを、ある一定の期間だけ復号可能とするコンテンツ伝送方法、伝送媒体、コンテンツ受信方法に関する。

【０００２】

【従来の技術】

放送やパッケージメディアからコンテンツを記録再生可能な記録再生装置において、コンテンツの著作権保護を目的として、様々なコンテンツの視聴制限が行われている。既にディジタル衛星放送では、ペイ・パー・デイ方式の番組が放送されている。この方式では、視聴者である一般ユーザは、決められた購入動作によって番組提供者に対価をを支払うことで、購入した日に限りその番組を何度でも視聴することができる。

【０００３】

また、記録媒体に記録したコンテンツにおいては、特開2000-149417号公報に開示されている再生済みのコンテンツであることを示すフラッグを立てることで、一回視聴可のコンテンツとすることができる。

【０００４】

【発明が解決しようとする課題】

しかし、従来のペイ・パー・デイ方式では、放送された番組をユーザがコンテンツ記録装置により記録媒体に記録した場合、ユーザは制限なく再視聴することが可能になる。

【０００５】

一方、この放送番組をコピーコントロールインフォメーションなどを使い記録不可番組とすると、正当に対価を支払い購入した番組でありながら、ユーザは記録再生装置を使って自分の見たいシーンだけを何度も見るといったことはできない。

【０００６】

また、ペイ・パー・デイ方式の番組放送だけでリアルタイムに視聴する場合、朝に番組を購入したユーザと、夜に番組を購入したユーザは、同じ対価を支払いながら、その番組を視聴できる回数は等しくないという矛盾が生じる。

【０００７】

本発明は以上の問題点を考慮し、暗号化され記憶されたコンテンツを、ある一定の期間だけ復号可能とするコンテンツ伝送方法、伝送媒体、コンテンツ受信方法を提供することを目的としている。

【０００８】

【課題を解決するための手段】

そこで、上記課題を解決するために本発明は、下記のコンテンツ伝送方法、伝送媒体、コンテンツ受信方法を提供するものである。

（１）　コンテンツの再生を許可することを示すコンテンツ再生許可情報を生成し、

生成された前記コンテンツ再生許可情報に少なくとも基づき鍵情報を生成し、

生成された前記鍵情報を元に前記コンテンツを暗号化し、

前記暗号化されたコンテンツと、前記暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを併せて伝送する、

ことを特徴とするコンテンツ伝送方法。

（２）　コンテンツの再生を許可することを示すコンテンツ再生許可情報に少なくとも基づき生成された鍵情報に基づいて暗号化されたコンテンツと、

前記暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報と、

を伝送することを特徴とする伝送媒体。

（３）　コンテンツの再生を許可することを示すコンテンツ再生許可情報に少なくとも基づき生成された鍵情報に基づいて暗号化されたコンテンツと、その暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを受信して、前記暗号化されたコンテンツを再生するコンテンツ受信方法であって、

受信した前記暗号化されたコンテンツと前記伝送日時情報とを記憶し、

記憶された前記暗号化されたコンテンツに対する再生要求がなされた時点からその暗号化されたコンテンツを復号するための鍵情報を生成する時点までの間における日時に関する再生日時情報を得、

記憶された前記伝送日時情報と、前記再生日時情報と、前記暗号化されたコンテンツの再生許可期限情報とに基づき、前記暗号化されたコンテンツの再生を許可することを示すコンテンツ再生許可情報を生成し、

生成された前記コンテンツ再生許可情報に少なくとも基づき前記鍵情報を生成し、

記憶された前記暗号化されたコンテンツを、生成された前記鍵情報を元に復号する、

ことを特徴とするコンテンツ受信方法。

（４）　上記（３）記載のコンテンツ受信方法において、

前記再生許可期限情報は予め設定されていることを特徴とするコンテンツ受信方法。

（５）　上記（３）記載のコンテンツ受信方法において、

前記再生許可期限情報は外部から供給される情報に基づき設定されることを特徴とするコンテンツ受信方法。

【０００９】

【発明の実施の形態】

本発明の記録装置と再生装置の第１実施例を図１を用いて説明する。記録装置１は、年月日（日付）と時刻を設定可能な時計２、時計２から必要な日時（日付と時刻）に関する情報を取得する日時情報取得部３、コンテンツを暗号化する暗号鍵（鍵情報）をコンテンツ再生許可情報と日時情報とを用いて生成する鍵情報生成部４、鍵情報生成部４で生成した暗号鍵（鍵情報）を用いてコンテンツを暗号化する暗号化部５と、暗号化したコンテンツと記録日時情報を併せて記録媒体７に記録する記録部６から構成される。ここで、記録日時情報とは、コンテンツのこの装置への入力時点から記録時点までの間における日時に関する情報、もしくは予め設定された記録日時情報である。

【００１０】

時計２は、年、月、日、時、分、秒、など日時に関する情報を設定することができる。日時情報取得部３では、時計で得られる情報の、年、月、日、時、分、秒をBCD（Binary Coded Decimal）コードとして処理する。但し、年情報は西暦として00から99年までを表すとして8ビット、月情報は1から12までで5ビット、日情報は1から31までで6までビット、時情報は0から23までで6ビット、分情報は0から59までで7ビット、秒情報は0から59まで7ビットとする。鍵情報生成部４では、まず次式を満たす1ビットのx：コンテンツ再生許可情報を求める。

【００１１】

$$x = f(CT-RT) \cdots\cdots\cdots\cdots \text{（式１）}$$

但し、関数f(y)は、y<Tまたはy=T（T>0）のときf(y)=0、y>Tのときf(y)=1とする。またCT、RTはそれぞれ現在日時と、記録日時とする。Tは後述する再生許可期限情報である。

次に、求めたxと記録日時情報に基づき、

x||(年情報)||(年情報)||(年情報)||(月情報)

||(日情報)||(時情報)||(分情報)||(秒情報)
＝(1ビット)||(8ビット)||(8ビット)||(8ビット)||(5ビット)
||(6ビット)||(6ビット)||(7ビット)||(7ビット)
＝(56ビット)
＝(暗号鍵)
として出力する。但し、このとき通常は現在日時と記録日時とは同一日時（同一の日付と同一の時刻）なので、予めx=f(CT-RT)=f(0)=0を、再生を許可することを示す値であるコンテンツ再生許可情報として、鍵情報の一部とする。
（なお、||記号は、8ビット$b_7b_6b_5b_4b_3b_2b_1b_0$とすると4ビット$b_7b_6b_5b_4$と4ビット$b_3b_2b_1b_0$とにおいて、
$b_7b_6b_5b_4b_3b_2b_1b_0 = b_7b_6b_5b_4 \,||\, b_3b_2b_1b_0$
を表すものとする。）

暗号化部５ではこの暗号鍵を用いて、DES暗号でコンテンツの暗号化を行う。暗号化したコンテンツデータd_iは、記録部６にて記録日時情報t_iと併せて記録媒体７に記録される。

【００１２】

このときコンテンツデータd_iはある一定時間L_tの映像、または音声の情報とし、一定時間L_tが経過したのちは、日時情報取得部３で時計より日時情報（記録日時情報）を取得し、鍵情報生成部４では新たに暗号鍵を生成する。その新たな暗号鍵により暗号化部５で暗号化したコンテンツは、コンテンツデータd_{i+1}として記録日時情報t_{i+1}（$=t_i+L_t$）と併せて記録部６にて記録媒体に記録される。

【００１３】

このとき記録媒体は、光ディスク、磁気テープ、固体メモリ、ハードディスクなどデジタルデータを記録できるものであればいずれであっても良い。

【００１４】

なお、ここでは一定時間L_t毎に時間ｔを記録するように説明したが、コンテンツの先頭を記録開始するときの日時情報のみを記録して、コンテンツの途中状態における記録日時情報は、コンテンツ内に記述されているタイムコード情報やシステムクロック情報から換算した値を用いても良い。例えばＭＰＥＧなどのデ

ータにはビデオのＧＯＰレイヤーにはタイムコードが記述されている。また、システムレイヤーにはＳＣＲ（システムクロックリファレンス）やＰＣＲ（プログラムクロックリファレンス）があり、９０ＫＨｚもしくは２７ＭＨｚのクロック精度でカウントされているカウント情報が記述されており、それらの情報を用いて、先頭の記録開始時点の日時情報に、経過時間を換算して加算することで換算することが可能になる。

【００１５】

次に再生装置８は、記録媒体７から暗号化されたコンテンツとその記録日時情報とを読み出す再生部９と、暗号化されたコンテンツを復号化する復号化部１３と、年月日（日付）と時刻とを設定可能な時計１０と、時計より日時情報（日付と時刻）を取得する日時情報取得部１１と、日時情報取得部１１にて取得した再生日時情報と再生部９により読み出した記録日時情報と再生許可期限情報とから復号化に使う復号鍵（鍵情報）を生成する鍵情報生成部１２から構成される。ここで、再生日時情報とは、暗号化されたコンテンツに対する再生要求がなされた時点から暗号化されたコンテンツを復号するための復号鍵（鍵情報）を生成する時点までの間における日時に関する情報である。

【００１６】

再生装置８では、まず、再生部９にて記録媒体７に記録されている暗号化されたコンテンツと、そのコンテンツが記録媒体に記録された日時に関する記録日時情報（もしくは予め設定された記録日時情報）とを読み出す。次に、復号鍵（鍵情報）を生成するために、記録装置１と同様にして、時計１０より日時情報取得部１１にて、現在の日時（再生日時）を取得する。

【００１７】

鍵情報生成部１２では、日時情報取得部１１にて取得した現在日時（再生日時）CTと記録媒体より読み出した記録日時RTより、前述の式（１）からx：コンテンツ再生許可情報を算出する。算出したxと記録日時情報の年、月、日、時、分、秒とより、記録装置１と同様にして56ビットの復号鍵を生成する。生成した復号鍵を用いて、復号化部１３ではDES暗号でコンテンツの復号化を行う。

【００１８】

このとき再生装置において、(CT-RT)が決められた再生許可期限情報Tの値以下のときは、コンテンツ再生許可情報x=0となりコンテンツ記録時と生成される鍵が同一となる。よってコンテンツは正しく再生される。一方、(CT-RT)が決められた再生許可期限情報Tの値より大きいときは、コンテンツ再生許可情報x=1となりコンテンツ記録時と生成される鍵が異なる。よってコンテンツは正しく再生されない。

【００１９】

このように、図１に示した実施例の記録装置、再生装置を用いれば、記録日時から再生日時までの期間が再生許可期限Tの値以内であるときのみ、コンテンツを視聴可能とすることができる。より詳しく表現すれば、図１に示した実施例の記録装置、再生装置を用いれば、暗号化されたコンテンツに対する記録媒体への記録動作が行われた日時に関する記録日時情報もしくは予め設定された記録日時情報から、暗号化され記録されたコンテンツに対する再生要求がなされた時点からその暗号化されたコンテンツを復号するための鍵情報を生成する時点までの間における日時に関する情報である再生日時情報までの時間時期間が、再生許可期限情報Tの値以内であるときのみコンテンツを視聴可能とすることができる。

【００２０】

なお、再生許可期限情報Tは予め再生装置内に設定されていても良いし、外部から供給される情報（例えば記録媒体に記録してある情報）に基づきコンテンツに応じて装置内にその都度設定されるものでも良い。

【００２１】

また、図１において記録部６を、暗号化されたコンテンツと、その暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを併せて伝送する伝送部とすれば（他の部分においても記録日時情報を伝送日時情報とする）、記録装置１は伝送装置に応用できる。この場合、記録媒体７を、暗号化されたコンテンツと、その暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを併せて伝送する伝送媒体とする。

【００２２】

図１に示す再生装置８も次のようにすれば受信装置に応用できる。再生部９を、暗号化されたコンテンツと、その暗号化されたコンテンツに対する伝送動作が行われた日時に関する伝送日時情報もしくは予め設定された伝送日時情報とを受信して、受信した前記暗号化されたコンテンツと前記伝送日時情報とを記憶する受信・記憶部とする。日時情報取得部１１は、記憶された前記暗号化されたコンテンツに対する再生要求がなされた時点からその暗号化されたコンテンツを復号するための鍵情報を生成する時点までの間における日時に関する再生日時情報を得るようにする。鍵情報生成部１２は、記憶された前記伝送日時情報と、日時情報取得部１１で得た前記再生日時情報と、前記暗号化されたコンテンツの再生許可期限情報Tとに基づき、前記暗号化されたコンテンツの再生を許可することを示すコンテンツ再生許可情報を生成し、そのコンテンツ再生許可情報から復号鍵を生成する。

【００２３】

ここで、再生許可期限情報Tは予め受信装置内に設定されていても良いし、外部から供給される情報（例えば伝送されてくる情報）に基づきコンテンツに応じて装置内にその都度設定されるものでも良い。再生許可期限情報Ｔの元になる情報が伝送されるデータに記述される記述方法としては、例えば、次のような方法がある。デジタル放送のようにMPEG２のシステム（ＴＳストリーム）を使用する場合には、ＰＭＴ（プログラムマップテーブル）の中に時限情報用のdescryptorを定義して、記述することができる。もしくはコンテンツの頭にヘッダーをつけてそこに記述する方法でも良い。受信装置はそのデータを検出して再生許可期限情報Ｔをセットするようにする。

【００２４】

次に、本発明の記録装置と再生装置の第２実施例を図２を用いて説明する。記録装置２１は、年月日（日付）と時刻を設定可能な時計２２、時計２２から必要な日時（日付と時刻）に関する情報を取得する日時情報取得部２３、コンテンツを暗号化する暗号鍵（鍵情報）を生成する鍵情報生成部２４、鍵のもとになる情報と記録日時情報を管理するメモリ管理部２７と、鍵のもとになる情報と記録日時情報とを関連づけて記憶するフラッシュメモリ２８と、鍵情報生成部２４で生

成した暗号鍵を用いてコンテンツを暗号化する暗号化部２５と、暗号化したコンテンツと記録日時情報を併せて記録媒体３１に記録する記録部２６から構成される。ここで、記録日時情報とは、コンテンツのこの装置への入力時点から記録時点までの間における日時に関する情報である。

【００２５】

時計２２は、年、月、日、時、分、秒、など日時に関する情報を設定することができる。日時情報取得部２３では、時計で得られる情報の、年、月、日、時、分、秒をBCD（Binary Coded Decimal）コードとして処理する。但し、年情報は西暦として00から99年までを表すとして8ビット、月情報は1から12までで5ビット、日情報は1から31までで6ビット、時情報は0から23までで6ビット、分情報は0から59までで7ビット、秒情報は0から59まで7ビットとする。

【００２６】

鍵情報生成部２４では、鍵のもとになる情報として乱数r_iを生成し、r_iをもとに暗号鍵を生成する。

【００２７】

乱数r_iは乱数r_iを生成した日時情報（記録日時情報に相当する情報）と併せてメモリ管理部２７に出力される。メモリ管理部２７はフラッシュメモリ２８に乱数r_iと日時情報t_iとを記憶させ管理する。フラッシュメモリ２８はここでは着脱自在のものとする。

【００２８】

生成した暗号鍵は暗号化部２５に出力される。暗号化部２５ではこの暗号鍵を用いて、DES暗号でコンテンツの暗号化を行う。記録部２６では、日時情報取得部２３により取得した乱数r_iを生成した日時情報t_iを記録日時情報とし、この記録日時情報t_iと暗号化したコンテンツデータd_iとを、併せて記録媒体３１に記録する。

【００２９】

このときコンテンツデータd_iはある一定時間L_tの映像、または音声の情報とし、一定時間L_tが経過したのちは、日時情報取得部２３で時計２２より日時情報（記録日時情報）を取得し、鍵情報生成部２４では新たに暗号鍵を生成する。その

新たな暗号鍵により暗号化部２５で暗号化したコンテンツは、コンテンツデータd_{i+1}として記録時刻t_{i+1}（$=t_i+L_t$）と併せて記録部２６にて記録媒体に記録される。

【００３０】

メモリ管理部２７では、フラッシュメモリ２８内の乱数r_iに関連づけられた日時情報（記録日時情報）t_iから一定期間が過ぎた乱数r_iを消去するか、または新しい乱数r_kとその日時情報t_kとに変更する。メモリ管理部２７は、日時情報（記録日時情報）t_iと、日時情報取得手段で取得した現在の日時に関する情報である現在日時情報とを比較する比較手段を有するものである。この比較手段により、日時情報（記録日時情報）t_iから所定の一定期間が経過したか否かを判断する。

【００３１】

記録部２６にてコンテンツ及び記録日時情報を記録する記録媒体３１は、光ディスク、磁気テープ、固体メモリ、ハードディスクのいずれであっても良い。

【００３２】

次に、再生装置４１は、記録媒体３１から暗号化されたコンテンツとその記録日時情報とを読み出す再生部４２と、暗号化されたコンテンツを復号化する復号化部４８と、年月日（日付）と時刻とを設定可能な時計４３と、時計４３より日時情報（日付と時刻）を取得する日時情報取得部４４と、日時情報取得部４４にて取得した現在日時情報と再生部４２により読み出した記録日時情報とをもとにフラッシュメモリ４６内の乱数r_iとその日時情報（記録日時情報に相当）t_iを管理するメモリ管理部４５と、乱数r_iとその日時情報t_iとを記憶したフラッシュメモリ４６と、フラッシュメモリの乱数r_iを鍵のもとになる情報として復号鍵を生成する鍵情報生成部４７とから構成される。ここで、フラッシュメモリ４６は、記録媒体３１への記録動作終了後に記録装置２１から外したフラッシュメモリ２８を再生装置４１に装着したものである。（記録装置２１と再生装置４１とが一体の記録再生装置であれば、フラッシュメモリは着脱式でなくとも共用できるので、固定式のものでも良い。）

再生装置４１では、まず再生部４２にて記録媒体３１に記録されている暗号化されたコンテンツと、そのコンテンツが記録媒体に記録された日時に関する記録

日時情報（この例では乱数r_iを生成した日時情報t_i）を読み出す。読み出した記録日時情報をもとにメモリ管理部４５では、その日時情報に対応する乱数を鍵のもとになる情報として鍵情報生成部４７に出力する。鍵情報生成部４７では復号鍵を生成し、復号化部４８に出力し、復号化部４８でコンテンツの復号化を行う。

【００３３】

もし、記録装置２１側でフラッシュメモリ２８が装着された状態で一定時間が経過したために、記録装置２１でフラッシュメモリ２８内の対応する乱数が消去もしくは変更されている場合は、当然再生装置４１に装着されたフラッシュメモリ４６内の対応する乱数が消去もしくは変更されているので、鍵のもとになる正しい情報が存在しないため、復号鍵が生成されずコンテンツは正しく再生されない。

【００３４】

また、現在日時情報を再生装置４１側の日時情報取得部４４で取得することで、メモリ管理部４５では、フラッシュメモリ４６内の乱数r_iに関連づけられた日時情報（記録日時情報）t_iから特定の一定期間が過ぎた乱数r_iを消去するか、または新しい乱数r_kとその時刻情報t_kとに変更する。メモリ管理部４５は、日時情報（記録日時情報）t_iと、日時情報取得部４４で取得した現在の日時に関する情報である現在日時情報とを比較する比較手段を有するものである。この比較手段により、日時情報（記録日時情報）t_iから特定の一定期間が経過したか否かを判断する。

【００３５】

この場合でも、ある特定の期間が経過した場合は、鍵のもとになる正しい情報がフラッシュメモリ４６内に存在しなくなるため、復号鍵が生成されずコンテンツを復号化できない。

【００３６】

このように、図２に示した第２実施例の記録装置、再生装置を用いれば、鍵のもとになる情報を消去または変更することで、記録媒体に記録されたコンテンツをある特定の期間のみ視聴可能とすることができる。

【００３７】

次に、本発明の記録装置と再生装置の第３実施例を図３に示す。

【００３８】

第２実施例においては、フラッシュメモリ内の鍵のもとになる情報（乱数r_i）と、その情報を元にした鍵により暗号化され記録されたコンテンツデータ部分とを対応づけるために、記録日時情報tを用いていた。この第３実施例は、図３に示すようにリンク情報l_iを用いて、フラッシュメモリ内の鍵のもとになる情報（乱数r_i）と、その情報を元にした鍵により暗号化され記録されたコンテンツデータ部分とを対応づける用にしたものである。即ち、暗号化したコンテンツデータd_i毎にリンク情報l_iを記録媒体３１ａに記録する。フラッシュメモリ２８ａにも、メモリ管理部２７ａにより乱数r_iと日時情報（記録日時情報）t_iとに関連させてリンク情報l_iを記録しておく。再生装置側では記録媒体３１ａからリンク情報l_iを読み出し、そのリンク情報に基づき、メモリ管理部４５ａにより、暗号化されているコンテンツデータとリンクする乱数r_iをフラッシュメモリ４６ａから読み出す。これにより、第２実施例と同様な動作が行える。

【００３９】

上記のリンク情報には、記録日時情報よりもビット数が十分に少ないものを用いることができる。従って、第３実施例のものは、第２実施例のものよりも記録効率を向上させることができる。

【００４０】

なお、上記各実施例では、時計で得られる情報の、年、月、日、時、分、秒を用いて日時情報を説明したが、時の流れのなかの１点を特定できる情報であればどんなものでも日時情報に用いることができる。

【００４１】

また、本発明により作成したデータを記録媒体に記録せずに、放送や通信などを用いて、伝送する伝送方法及び装置にも適用できる。また、同様に記録媒体から再生するだけでなく、放送や通信などのインフラから本発明により作成したデータを受信する受信方法及び受信装置にも適用できる。このような機能をもつ電子データがハードディスクサーバーなどに多数記録されている状態における電子

データ、ならびに伝送されいている状態の伝送媒体にも適用できる。また、暗号方法はDES暗号に限らず他の共通鍵暗号方式、あるいは公開鍵暗号方式で適用できる。鍵生成において、鍵のもとになる情報は時刻情報あるいは乱数以外のパラメータであっても良い。また図２でのフラッシュメモリ内の鍵のもとになる情報とコンテンツデータとの対応は時刻情報ではなく、他の対応関係を示す情報であっても良い。

【００４２】

ここで、本特許を用いて所定の時間で復号を不可能とする記録装置、再生装置、伝送装置、受信装置を実現できるが、例えば、時計に設定されている日時を現在日時より前に戻すなどして、つねに復号可となるような改ざんが行われる恐れがある。

【００４３】

このようなことを避けるために、時計が外的要因によって変更された場合、またはコンテンツデータと併せて記録した記録日時情報が不正に変更された場合、または、各装置内の鍵情報生成部、暗号化部、復号化部など暗号に関する部分が不正に解読または変更された場合には、暗号鍵のもとになる情報の少なくとも一部が変化するパラメータを予め用意しておくことがより好ましい。

【００４４】

例えば、その鍵のもとになる情報は、電源投入時または記録開始時に生成される乱数とし、その乱数は所定の揮発性メモリに記録されるとする。メモリ内の乱数は、電源切りの場合、時計が外的要因により不正に変更された場合、所定の時間が経過した場合、コンテンツデータと併せて記録した記録日時情報が不正に変更もしくはアクセスされた場合に、消去もしくは新たな乱数に変更されるものとする。これにより、もし時計の不正な変更、記録媒体上のデータの改ざん、各装置の改造または解析のいすれかが行われれば、正しい復号鍵が得られず、コンテンツを復号化できなくすることができる。

【００４５】

次に、暗号化され記録されたコンテンツを、ある一定の期間だけ復号可能とするコンテンツ記録装置、コンテンツ再生装置の他の例を図４に示す。

【００４６】

記録装置は、年月日と時刻情報を設定可能な時計、時計から必要な日時に関する情報を取得する時刻情報取得部、コンテンツを暗号化する暗号鍵を時刻情報から生成する鍵情報生成部、鍵情報生成部で生成した暗号鍵を用いてコンテンツを暗号化する暗号化部から構成される。

【００４７】

時計は、年、月、日、時、分、秒、など日時に関する情報を設定することができる。時刻情報取得部では、時計で得られる情報の中から、年、月、日をBCD（Binary Coded Decimal）コードとして処理する。但し、年情報は西暦として00から99年までを表すとして8ビット、月情報は1から12までで5ビット、日情報は1から31までで6ビットとする。暗号化部での暗号化方式を共通鍵暗号のDES暗号とすれば、必要な暗号鍵のビットサイズは64ビットである。但し8ビットはパリティビットである。鍵情報生成部では、

(年情報)||(月情報)||(月情報)||(月情報)||(月情報)
||(月情報)||(月情報)||(日情報)||(日情報)||(日情報)
＝(8ビット)||(5ビット)||(5ビット)||(5ビット)||(5ビット)
||(5ビット)||(5ビット)||(6ビット)||(6ビット)||(6ビット)
＝(56ビット)
＝（暗号鍵）

として出力する。

【００４８】

暗号化部ではこの暗号鍵を用いて、DES暗号でコンテンツの暗号化を行う。暗号化したコンテンツは、記録部にて記録媒体に記録される。このとき記録媒体は、光ディスク、磁気テープ、固体メモリ、ハードディスクなどデジタルデータを記録できるものであればいずれであっても良い。

【００４９】

再生装置は、記録媒体より暗号化したコンテンツを読み出す再生部と、暗号化したコンテンツを復号化する復号化部と、その復号化に使う復号鍵を生成する鍵情報生成部と、鍵情報を生成するもとになる情報として、時計より時刻情報を取

得する時刻情報取得部、年月日と時刻情報を設定可能な時計から構成される。

【００５０】

再生装置では、まず再生部にて記録媒体に記録されたコンテンツを読み出す。記録装置と同様にして、時計、時刻情報取得部、鍵情報生成部より、コンテンツ復号化の56ビットの鍵を得る。得られた鍵を用いて、復号化部ではDES暗号でコンテンツの復号化を行う。このとき、年、月、日いずれかの情報の少なくとも一つが、記録時と異なれば、鍵情報生成部から得られる復号鍵は暗号鍵と異なり、コンテンツは正しく再生されない。このように、図４に示した記録装置、再生装置を用いれば、ある特定の年月日にのみコンテンツを視聴可能とすることができる。

【００５１】

次に、暗号化され記録されたコンテンツを、ある一定の期間だけ復号可能とするコンテンツ記録装置、コンテンツ再生装置のさらに他の例を図５に示す。

【００５２】

記録装置は年月日と時刻情報を設定可能な時計、時計から必要な日時に関する情報を取得する時刻情報取得部、コンテンツを暗号化する暗号鍵を生成する鍵情報生成部、鍵情報生成部で生成した暗号鍵を用いてコンテンツを暗号化する暗号化部と、暗号化したコンテンツと記録時刻情報を併せて記録媒体に記録する記録部から構成される。

【００５３】

時計は、年、月、日、時、分、秒、など日時に関する情報を設定することができる。時刻情報取得部では、時計で得られる情報の、年、月、日、時、分、秒をBCD（Binary Coded Decimal）コードとして処理する。但し、年情報は西暦として00から99年までを表すとして8ビット、月情報は1から12までで5ビット、日情報は1から31までで6ビット、時情報は0から23までで6ビット、分情報は0から59までで7ビット、秒情報は0から59まで7ビットとする。鍵情報生成部では、再生側と同じ56ビットの鍵を出力する。

【００５４】

暗号化部ではこの暗号鍵を用いて、DES暗号でコンテンツの暗号化を行う。暗

号化したコンテンツデータd_iは、記録部で時刻情報取得部にて取得した時刻情報を記録時刻情報t_iとして併せて記録媒体に記録する。このときコンテンツデータd_iはある一定時間L_tの映像、または音声の情報とし、L_tが経過したのちは、時刻情報取得部で時計より時刻情報を取得し、暗号化部で暗号化したコンテンツは、コンテンツデータdi+1として記録時刻t_{i+1}（$=t_i+L_t$）と併せて記録部にて記録媒体に記録される。このとき記録媒体は、光ディスク、磁気テープ、固体メモリ、ハードディスクのいずれであっても良い。

【００５５】

再生装置は、記録媒体より暗号化したコンテンツとその記録時刻を読み出す再生部と、暗号化したコンテンツを復号化する復号化部と、年月日と時刻情報を設定可能な時計と、時計より時刻情報を取得する時刻情報取得部と、取得した時刻情報と再生部より読み出した記録時刻情報とを比較する比較部と、比較部の結果に応じて復号化部でのコンテンツの復号化を停止する制御部と、復号化に使う復号鍵を生成する鍵情報生成部から構成される。

【００５６】

再生装置では、まず再生部にて記録媒体に記録されたコンテンツとそのコンテンツの記録時刻情報を読み出す。読み出した記録時刻情報は、時計から時刻情報取得部にて得られる現在時刻と、時刻情報比較部にて比較される。比較は現在時刻と記録時刻との差を求める。復号化制御部では、比較部にて求めた現在時刻と記録時刻の差がある特定の値T以上の場合、復号化部でのコンテンツの復号化を停止する。

【００５７】

このように、図５に示した記録装置と再生装置を用いれば、再生側の制御部での特定の値Tを設定することで、記録媒体に記録されたコンテンツを決められた期間内のみコンテンツを視聴可能とすることができる。

【００５８】

【発明の効果】

以上の通り、本発明のコンテンツ伝送方法、伝送媒体、コンテンツ受信方法を用いれば、暗号化され記録されたコンテンツを、ある一定の期間だけ復号可能と

することが可能となる。コンテンツの利用者側において一度記録したコンテンツに対してある一定の期間（コンテンツ権利者側の意図する期間内）だけ復号可能とできることは、コンテンツの利用者が各自の都合の良い時間帯（もちろん前記一定の期間内における都合の良い時間帯）においてコンテンツを利用可能とすると共に、記録されたコンテンツの著作権等を保護できるという利用者側とコンテンツ権利者側との両者にとって非常に有益なものである。

【図面の簡単な説明】

【図１】

第１実施例のブロック構成図である。

【図２】

第２実施例のブロック構成図である。

【図３】

第３実施例のブロック構成図である。

【図４】

他の実施例を示す図である。

【図５】

他の実施例を示す図である。

【符号の説明】

１　記録装置

２　時計

３　日時情報取得部

４　鍵情報生成部

５　暗号化部

６　記録部

７　記録媒体

８　再生装置

９　再生部

１０　時計

１１　日時情報取得部

１２　鍵情報生成部

１３　復号化部

【書類名】　図面

【図１】

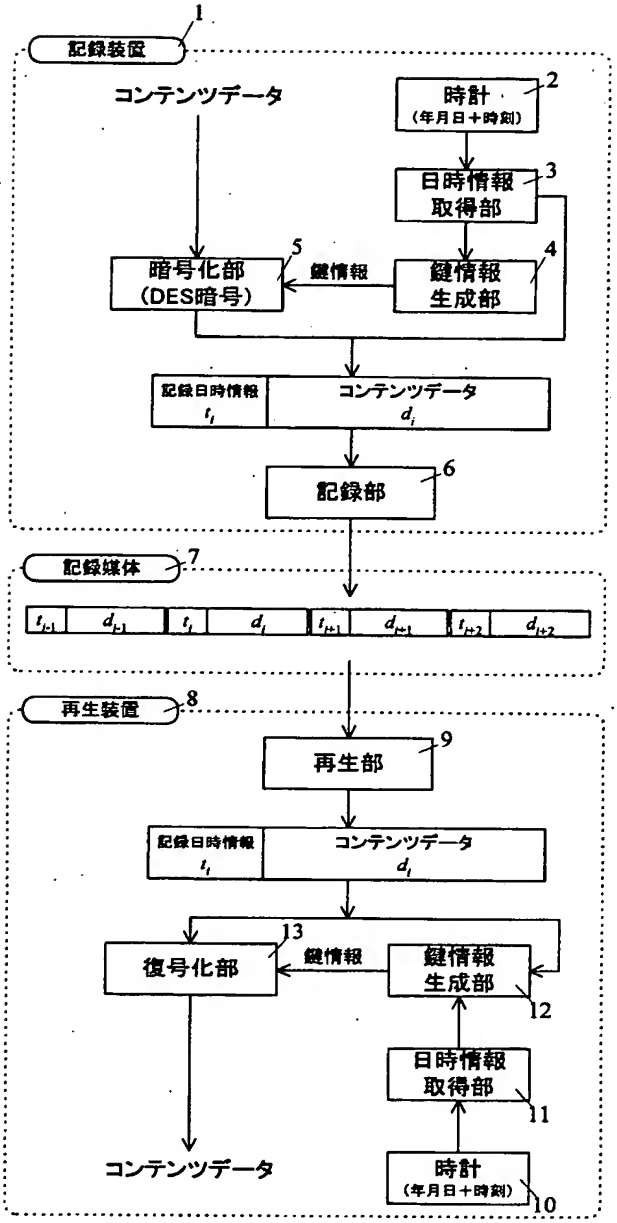
1
記録装置
コンテンツデータ
時計
(年月日＋時刻)
2
日時情報
取得部
3
暗号化部
(DES暗号)
5
鍵情報
鍵情報
生成部
4
記録日時情報
t_i
コンテンツデータ
d_i
記録部
6
記録媒体
7
t_{i-1} d_{i-1} t_i d_i t_{i+1} d_{i+1} t_{i+2} d_{i+2}
再生装置
8
再生部
9
記録日時情報
t_i
コンテンツデータ
d_i
13
復号化部
鍵情報
鍵情報
生成部
12
日時情報
取得部
11
コンテンツデータ
時計
(年月日＋時刻)
10

図1

【図２】

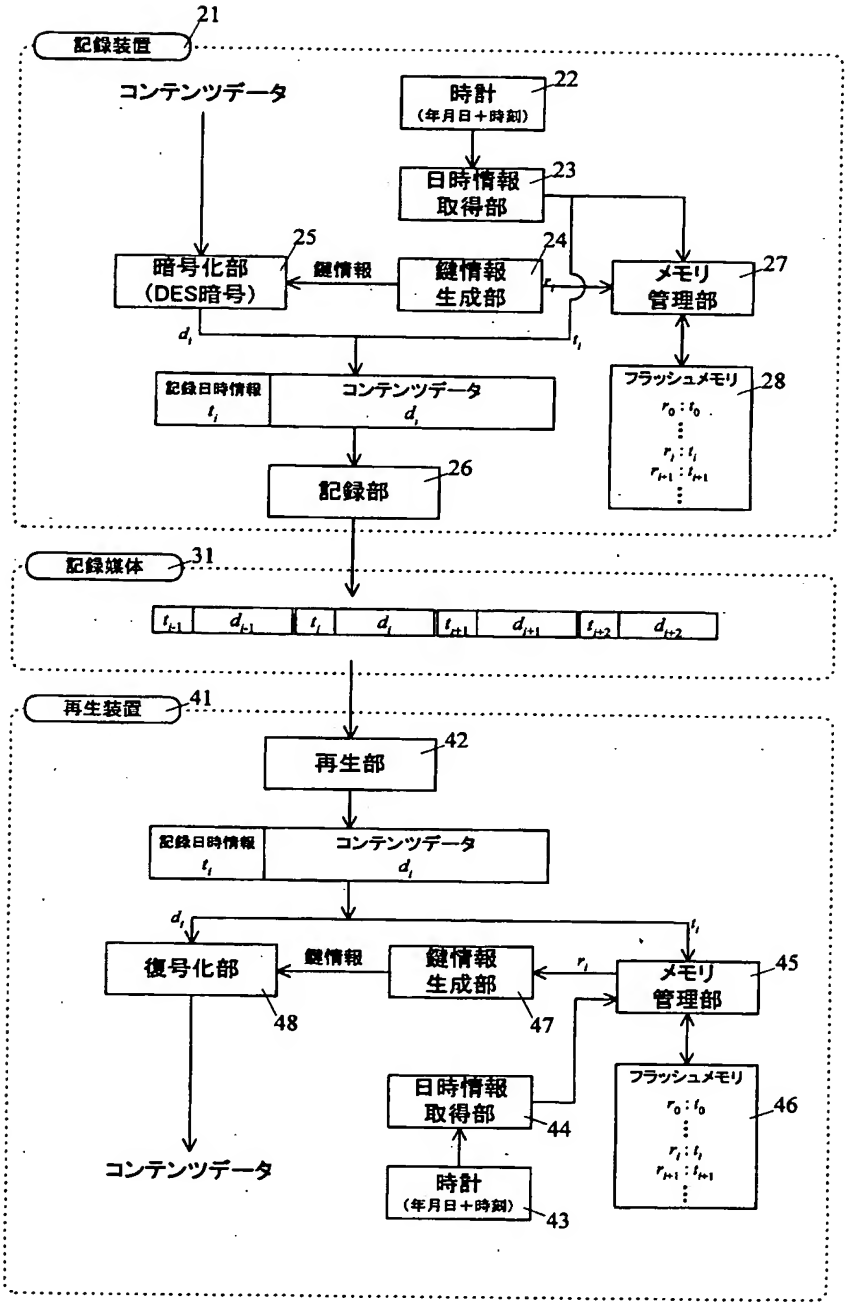
21
記録装置
コンテンツデータ
時計
(年月日＋時刻)
22
日時情報
取得部
23
暗号化部
(DES暗号)
25
鍵情報
鍵情報
生成部
24
メモリ
管理部
27
記録日時情報
コンテンツデータ
フラッシュメモリ
28
記録部
26
記録媒体
31
再生装置
41
再生部
42
記録日時情報
コンテンツデータ
復号化部
鍵情報
鍵情報
生成部
メモリ
管理部
45
48
47
日時情報
取得部
44
フラッシュメモリ
46
コンテンツデータ
時計
(年月日＋時刻)
43

図2

【図３】

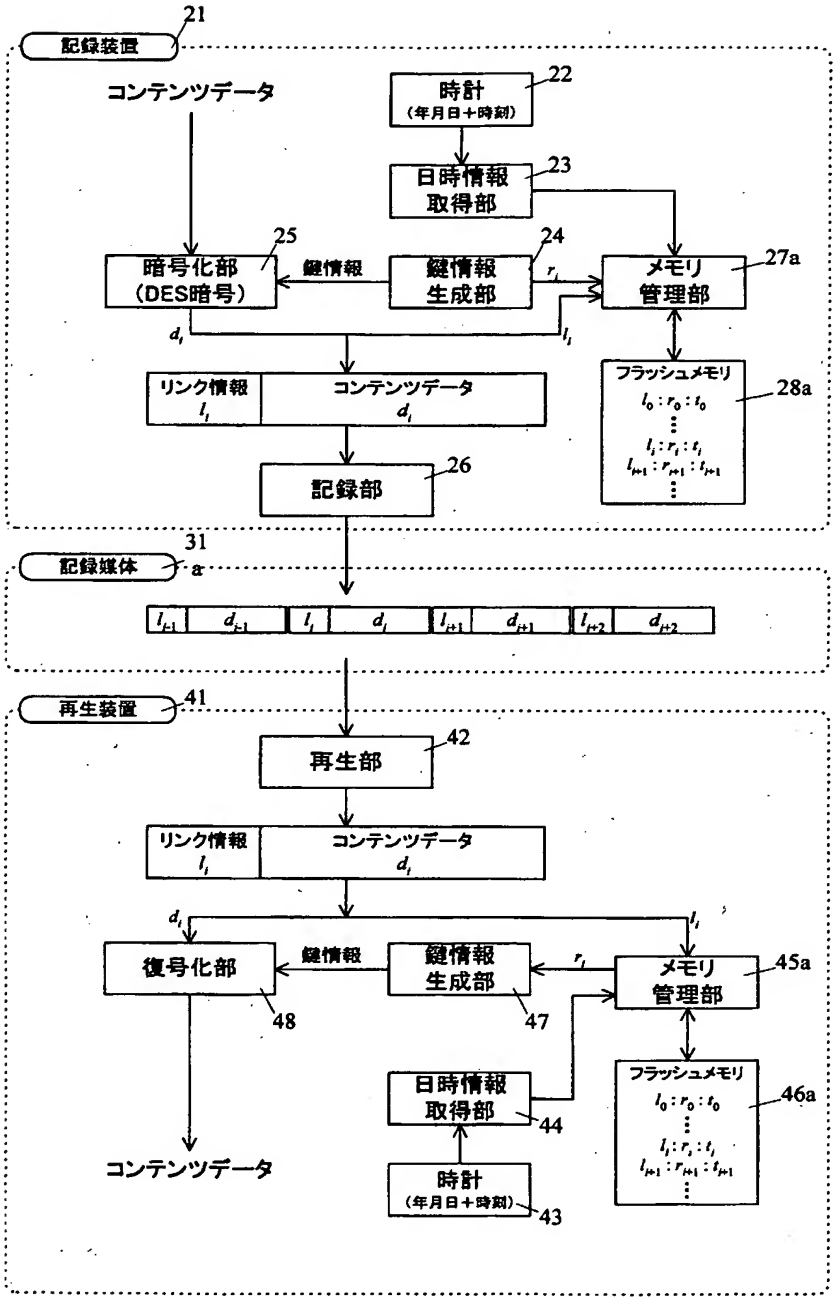
21
記録装置
コンテンツデータ
時計
（年月日＋時刻）
22
日時情報
取得部
23
25
暗号化部
（DES暗号）
鍵情報
24
鍵情報
生成部
r_i
メモリ
管理部
27a
d_i
l_i
リンク情報
l_i
コンテンツデータ
d_i
フラッシュメモリ
$l_0 : r_0 : t_0$
$l_i : r_i : t_i$
$l_{i+1} : r_{i+1} : t_{i+1}$
28a
記録部
26
31
記録媒体
l_{i-1} d_{i-1} l_i d_i l_{i+1} d_{i+1} l_{i+2} d_{i+2}
41
再生装置
再生部
42
リンク情報
l_i
コンテンツデータ
d_i
d_i
l_i
復号化部
鍵情報
鍵情報
生成部
r_i
メモリ
管理部
45a
48
47
日時情報
取得部
44
フラッシュメモリ
$l_0 : r_0 : t_0$
$l_i : r_i : t_i$
$l_{i+1} : r_{i+1} : t_{i+1}$
46a
コンテンツデータ
時計
（年月日＋時刻）
43

図3

【図４】

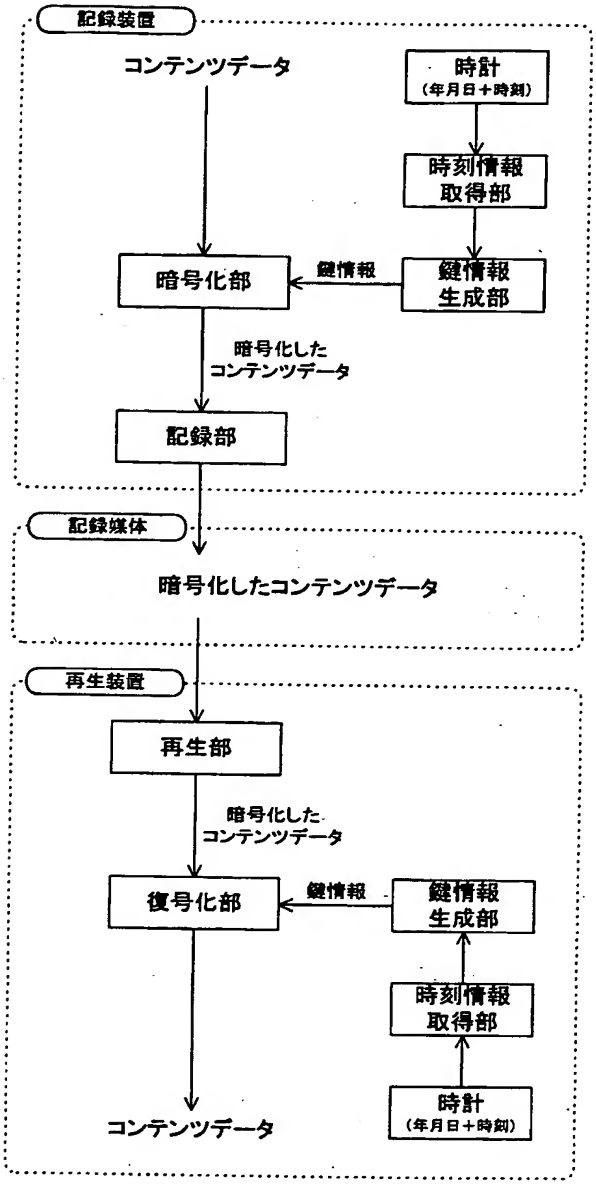
記録装置
コンテンツデータ
時計
（年月日＋時刻）
時刻情報
取得部
暗号化部
鍵情報
鍵情報
生成部
暗号化した
コンテンツデータ
記録部
記録媒体
暗号化したコンテンツデータ
再生装置
再生部
暗号化した
コンテンツデータ
復号化部
鍵情報
鍵情報
生成部
時刻情報
取得部
時計
（年月日＋時刻）
コンテンツデータ

図4

【図５】

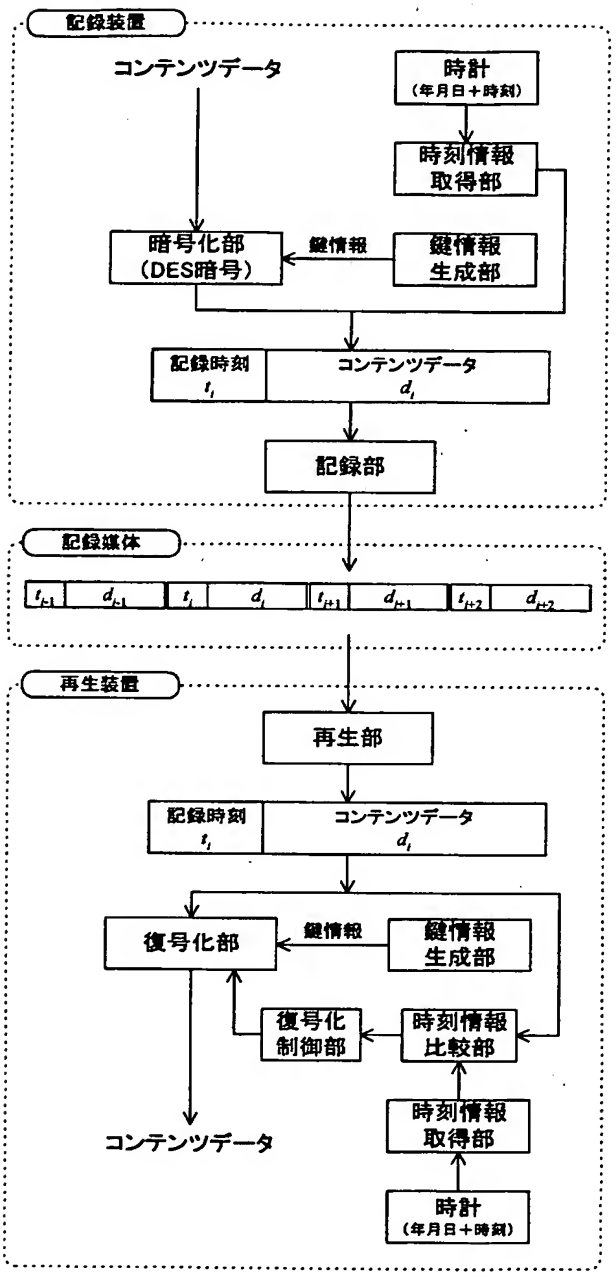
記録装置
コンテンツデータ
時計
（年月日＋時刻）
時刻情報
取得部
暗号化部
（DES暗号）
鍵情報
鍵情報
生成部
記録時刻
t_i
コンテンツデータ
d_i
記録部
記録媒体
t_{i-1} d_{i-1} t_i d_i t_{i+1} d_{i+1} t_{i+2} d_{i+2}
再生装置
再生部
記録時刻
t_i
コンテンツデータ
d_i
復号化部
鍵情報
鍵情報
生成部
復号化
制御部
時刻情報
比較部
時刻情報
取得部
時計
（年月日＋時刻）
コンテンツデータ

図5

【書類名】　　要約書

【要約】

【課題】　暗号化され記録されたコンテンツを、ある一定の期間だけ復号可能とする。

【解決手段】　コンテンツ再生許可情報に少なくとも基づき鍵情報を生成し、鍵情報を元にコンテンツを暗号化し、暗号化されたコンテンツと伝送日時情報とを併せて伝送する。受信側では、受信した暗号化されたコンテンツと伝送日時情報とを記憶し、記憶された暗号化されたコンテンツに対する再生日時情報を得、記憶された伝送日時情報と、前記再生日時情報と、暗号化されたコンテンツの再生許可期限情報とに基づき、暗号化されたコンテンツの再生を許可することを示すコンテンツ再生許可情報を生成する。そのコンテンツ再生許可情報に少なくとも基づき鍵情報を生成し、記憶された暗号化されたコンテンツを復号する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社